UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,966	06/30/2006	Hideo Sato	09792909-6649	3198

26263 7590 08/23/2010

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, WILLIS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
PHAM, QUANG	
ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
08/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/596,966	SATO, HIDEO	
	Examiner	Art Unit	
	QUANG PHAM	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 August 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/03/2010 has been entered.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1-2, 4-6, and 9-10 are rejected under 35 USC 103(a) as being unpatentable over Yap et al. (Yap – US 6,111,506) in view of Kono et al. (Kono – US 6,813,010 B2) and further in view of Bridgelall (Bridgelall – US 6,672,512 B2).**

(1). As to **claim 1**, **Yap** discloses method of making an improved security identification document including contactless communication insert unit. Further, **Yap** discloses *an information processing system comprising:*

a first information processing apparatus (FIG. 7 the improved security document 10) *and a second information processing apparatus* (FIG. 7 the improved security identification document interface unit 62), *said first information processing apparatus comprising:*

a storage (column 4 line 64 – column 5 line 6, column 12 lines 39-42 and FIG. 1; the microprocessor 14 function that would access memory/storage) *means which stores a first biological identification data associated with a predetermined portion of a subject's living body* (column 4 lines 38-53 and column 6 lines 45-51)*; and*

a first communication means for performing communication when held proximate to the predetermined portion of the subject's living body (column 15 lines 6-13, column 15 lines 31-37, column 5 line 64 – column 6 line 16)*, and*

the second information processing apparatus (FIG. 7 the improved security identification document interface unit 62) *comprising:*

a biological sensor (FIG. 7 the biometric data input device 72) *which detects biological information from the subject's living body* (column 15 lines 38-52 and FIG. 7)*;*

a second communication means which communicates with the first communication means (column 15 lines 20-37)*;* and

a biological authentication means which performs biological authentication (column 15 lines 56-65 and column 16 lines 6-11)*, based on the second biological identification data* (column 15 lines 38-52 and FIG. 7) *and on the first biological identification data* (column 4 lines 38-53 and column 6 lines 45-51)*;*

except for the claimed limitations of *an extraction means which extracts a second biological identification data from the biological information detected by the biological sensor while the first communication means transmits the first biological information to the second communication means.*

In **Yap**'s teaching, it would have been obvious to one skilled in the art at the time of the claimed invention that the user of the security identification document would/could well be using his/her hand to present the card for reading (inspected or validated proximate to or equipped on a predetermined portion of the subject's living body) and the same hand be used for scanning the biometric identification data (finger print scanning) for verification, for user convenience.

In the art of performing personal identification, **Kono** discloses a personal identification system wherein the system comprises a camera having a light source used to capture the person's blood vessel pattern, and the captured image is processed to extract identification data from the captured image (column 2, line 68 – column 3 lines 21 and FIG. 11 steps 1004-1103).

In the art of performing personal identification, **Bridgelall** discloses a system/method for a combined biometric reader (column 3 lines 56 – column 4 lines 9, column 6 lines 33-52, and FIG. 1 the barcode scanner 102 and the laser detection device 104) and RFID circuit (FIG. 1 the RFID circuit 106) to read the information from the RFID badge and finger print for authentication (column 3 lines 40-55, column 4 lines 62 – column 5 lines 12, and column 6 lines 33-52). Further, **Bridgelall** discloses the system can simultaneously process the biometric data signals and the RFID signals (abstract, column 4 lines 62 – column 5 lines 12, column 5 lines 56-62, column 6 lines 33-52, and FIG. 1).

In view of the teachings by **Yap, Kono** and **Bridgelall**, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *an extraction means which extracts a second biological identification data from the biological information detected by the biological sensor,* as taught by **Kono**, *while the first communication means transmits the first biological information to the second communication means*, as taught by

Bridgelall, in the personal identification system of **Yap**, for the purpose of identifying the captured biological data before performing the biological authentication process in a speedy, therefore convenient manner to the user.

(2). As to **claim 2**, **Yap** discloses method of making an improved security identification document including contactless communication insert unit. Further, **Yap** discloses *an information processing apparatus comprising:*

a biological sensor (FIG. 7 the biometric data input device 72) *which detects biological information from a living body* (column 15 lines 38-52 and FIG. 7) *when held proximate to a predetermined position of the living body;*

a communication target which stores biological identification data (column 4 lines 38-53, column 6 lines 45-51, and FIG. 7 the improved security document 10)*;*

a near-distance communication means which communicates with the communication target (column 5 line 64 – column 6 line 16, column 15 lines 6-11, and FIG. 7 the improved security document 10 as communication target)*;*

Except for the claimed limitations of *an extraction means which extracts biological identification data from the biological information detected by the biological sensor while the communication target transmits the stored biological identification data to the second communication means; and a biological authentication means which compares the stored biological identification data with the detected biological identification data.*

In **Yap**'s teaching, it would have been obvious one skilled in the art that the user of the security identification document would/could well be using his/her hand to present the card for reading (inspected or validated proximate to or equipped on a predetermined portion of the

subject's living body) and the same hand be used for scanning the biometric identification data (finger print scanning) for verification, for user convenience.

In the art of performing personal identification, **Kono** discloses a personal identification system wherein the system comprises a camera having a light source used to capture the person blood vessel pattern when the user fingers exposed to the light source, and the captured image is processed to identify the captured data (column 2 line 67 – column 3 lines 21, lines 36-40, FIG. 3A, FIG. 4, FIG. 7-9, and FIG. 11 steps 1004-1103).

In the art of performing personal identification, **Bridgelall** discloses a system/method combined biometric reader (column 3 lines 56 – column 4 lines 9, column 6 lines 33-52, and FIG. 1 the barcode scanner 102 and the laser detection device 104) and RFID circuit (FIG. 1 the RFID circuit 106) to read the information from the RFID badge and finger print for authentication (column 3 lines 40-55, column 4 lines 62 – column 5 lines 12, and column 6 lines 33-52). Further, **Bridgelall** discloses system can simultaneously process the biometric data signals and the RFID signals (abstract, column 4 lines 62 – column 5 lines 12, column 5 lines 56-62, column 6 lines 33-52, and FIG. 1).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *an extraction means which extracts biological identification data from the biological information detected by the biological sensor*, as taught by **Kono**, *while the communication target transmits the stored biological identification data to the second communication means*, as taught by **Bridgelall**, *and a biological authentication means which compares the stored biological identification data with the detected biological identification*

data, as taught by **Kono**, in the personal identification system of **Yap**, for the purpose of identifying the captured biological data before performing the biological authentication process.

(3). As to **claim 4**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 2** except for the claimed limitations of *the information processing apparatus further comprising: network communication means which communicates with a management server which manages the biological identification data registered in the communication target, establishing a correspondence thereof, wherein the biological authentication means compares mutually one another of the biological data at the predetermined portion, extracted by the extraction means, the biological identification data obtained from the management server via the network communication means, and the biological identification data obtained from the communication target via the near-distance communication means.*

In the art of performing personal identification, **Kono** discloses a personal identification system wherein the system comprises network communication means which communicates with a management server which manages the biological identification data registered in the communication target (column 5 lines 15-17, lines 22-27 and FIG. 10 steps 1000-1001 and database 100), establishing a correspondence thereof, wherein the biological authentication means compares mutually one another of the biological data at the predetermined portion (column 5 lines 27 – 42 and FIG. 10 steps 1002-1010), extracted by the extraction means, the biological identification data obtained from the management server via the network communication means (column 2 line 68 – column 3 lines 21 , column 5 lines 14-42, FIG. 10 step 1003, and FIG. 11 steps 1004-1103).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the information processing apparatus further comprising network communication means which communicates with a management server which manages the biological identification data registered in the communication target, establishing a correspondence thereof, wherein the biological authentication means compares mutually one another of the biological data at the predetermined portion, extracted by the extraction means, the biological identification data obtained from the management server via the network communication means, and the biological identification data obtained from the communication target via the near-distance communication means*, as taught by **Kono**, in the personal identification system of **Yap** and **Bridgelall**, for the purpose of developing a personal identification system including the database to mange all the registered users.

(4). As to **claim 5**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 2** except for the claimed limitations of *the information processing apparatus further comprising network communication means which communicates with a management server via a predetermined network, the management server managing the biological identification data registered in the communication target* (**Kono**: column 5 lines 15-17, lines 22-27 and FIG. 10 steps 1000-1001 and database 100) *and compressed data by use of data obtained in a process up to generation of the biological identification data, with a correspondence established between the biological identification data and a compressed data* (**Kono**: column 5 lines 27 – 42 and FIG. 10 steps 1002-1010), *wherein: the extraction means generates the compressed data by use of data obtained in a process up to extraction of the biological data at the predetermined portion from the biological data detected by the biological sensor; and the biological authentication means*

compares the compressed data generated by the extraction means with the compressed data obtained from the management server via the network communication means.

In the same art of performing personal identification, **Kono** discloses a personal identification system wherein the registered biological data is stored in the database during the registration (column 5 lines 15-17, lines 22-27 and FIG. 10 steps 1000-1001 and database 100). During the authentication process, the biological data obtained from the user using the imaging device (column 2 line 68 – column 3 lines 21, column 5 lines 14-42, FIG. 3A, FIG. 4, FIG. 7-9, FIG. 10 step 1003, and FIG. 11 steps 1004-1103) is compared to the registered biological data selected from the data (column 5 lines 17-21, lines 27-42 and FIG. 10 steps 1002-1010).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the extraction means generates the compressed data by use of data obtained in a process up to extraction of the biological data at the predetermined portion from the biological data detected by the biological sensor; and the biological authentication means compares the compressed data generated by the extraction means with the compressed data obtained from the management server via the network communication means,* as taught by **Kono**, in the individual personal identification system of **Yap** and **Bridgelall**, for the purpose of performing the biological authentication using the registered biological data stored in the database of the system with the biological obtain from user during the authentication process.

(5). As to **claim 6**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 5**. Further, **Yap** discloses *the biological data at the predetermined portion, extracted by the extraction means, with the biological identification data obtained from the communication target via the near-distance communication means* (column 4 lines 38-53, column 5 line 64 – column 6

line 16, lines 45-51, column 15 lines 20-37, lines 38-52 , lines 56-65, column 16 lines 6-11, and FIG. 7) except for the claimed limitations of *the information processing apparatus wherein the biological authentication means compares the compressed data generated by the extraction means with the compressed data obtained from the management server via the network communication means.*

In the same art of personal authentication, **Kono** discloses *the biological authentication means compares the compressed data generated by the extraction means with the compressed data obtained from the management server via the network communication means* (column 2 line 68 – column 3 lines 21, column 5 lines 14-42, FIG. 3A, FIG. 4, FIG. 7-9, FIG. 10 step 1000-1001, step 1003, database 100, and FIG. 11 steps 1004-1103).

Therefore it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the information processing apparatus wherein the biological authentication means compares the compressed data generated by the extraction means with the compressed data obtained from the management server via the network communication means,* as taught by **Kono**, in the personal identification system of **Yap** and **Bridgelall**, for the purpose of performing the double authentication between the card terminal, user, and the registered biological data stored in the management server to improve more security for the system.

(6). As to **claim 9**, **Yap** discloses method of making an improved security identification document including contactless communication insert unit. Further, **Yap** discloses *an information processing apparatus comprising:*

equipment means which is equipped on a predetermined portion of a living body (column 15 lines 6-13 and FIG. 7 the document 10) *and has (1) a storage* (column 4 line 64 – column 5

line 6, column 12 lines 39-42 and FIG. 1 the microprocessor 14) *means which stores a first biological identification data associated with the predetermined portion of the living body* (column 4 lines 38-53 and column 6 lines 45-51)*; and (2) a communication means which is held by the equipment means and transmits the first biological identification data directly to a communication target to which the predetermined portion equipped with the equipment means is brought close* (column 15 lines 6-13, column 15 lines 31-37, column 5 line 64 – column 6 line 16)*, and*

a biological authentication means which performs biological authentication (column 15 lines 56-65 and column 16 lines 6-11)*, based on the first biological identification data* (column 4 lines 38-53 and column 6 lines 45-51) *and on a second biological identification data* (column 15 lines 38-52 and FIG. 7).

Except for the claimed limitations of *said second biological identification data being extracted from biological information detected by a biological sensor while the communication means transmits the first biological identification data to the communication target.*

As **Yap**'s teaching, it is obvious that the user of the improved security identification document is using his/her hand to present the card for reading (inspected or validated proximate to or equipped on a predetermined portion of the subject's living body) and the same hand is being used for scanning the biometric identification data for verification.

In the art of performing personal identification, **Kono** discloses a personal identification system wherein the system comprises a camera having a light source used to capture the person blood vessel pattern, and the captured image is processed to identify the captured data (column 2 lines 68 – column 3 lines 21 and FIG. 11 steps 1004-1103).

In the art of performing personal identification, **Bridgelall** discloses a system/method combined biometric reader (column 3 lines 56 – column 4 lines 9, column 6 lines 33-52, and FIG. 1 the barcode scanner 102 and the laser detection device 104) and RFID circuit (FIG. 1 the RFID circuit 106) to read the information from the RFID badge and finger print for authentication (column 3 lines 40-55, column 4 lines 62 – column 5 lines 12, and column 6 lines 33-52). Further, **Bridgelall** discloses system can simultaneously process the biometric data signals and the RFID signals (abstract, column 4 lines 62 – column 5 lines 12, column 5 lines 56-62, column 6 lines 33-52, and FIG. 1).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include the extraction used to extract biological identification data from the biological information detected by the biological sensor , as taught by **Kono**, while the communication means transmits the first biological identification data to the communication target, as taught by **Bridgelall**, in the personal identification system of **Yap**, for the purpose of identifying the captured biological data before performing the biological authentication process.

(7). As to **claim 10**, **Yap**, **Kono,** and **Bridgelall** disclose limitations of **claim 9**. Further, **Yap** discloses *the information processing apparatus further comprising voltage accumulation means which accumulates a voltage induced in response to reception of a signal supplied from the communication target* (FIG. 1 the improved security identification document 10), *wherein the communication means transmits the biological identification data to the communication target, using the voltage accumulated by the voltage accumulation means as an electromotive force* (column 13 lines 3-25, column 15 lines 6-13, lines 21-24, and FIG. 1 the improved security identification document 10).

3. **Claim 3 is rejected under 35 USC 103(a) as being unpatentable over Yap in view of Kono, Bridgelall and further in view of Benhammou et al. (Benhammou – US 2004/0059925 A1).**

As to **claim 3**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 2** except for the claimed limitations of *the information processing apparatus further comprising: network communication means which communicates with a management server managing the communication target, via a predetermined network; and relay means which relays mutual authentication between the communication target and the management server via the network communication means and the near-distance communication means, wherein in accordance with a result of the mutual authentication, comparison is performed by the biological authentication means, or in accordance with a comparison result by the biological authentication means, the mutual authentication is relayed by the relay means.*

In the art of performing personal identification, **Kono** discloses a personal identification system wherein the system comprises database to manage the user registered information (the user registered finger-vein) (column 5 lines 15-17, lines 22-27 and FIG. 10 steps 1000-1001 and database 100). During the authentication process, by obtaining the user ID from the user input in a non contact device for instance from the information stored on the IC card issued to the user (column 7 line 62 – column 8 line 5), the user registered image is selected from the database and compared to the captured image obtained from user hand; the biological authentication is performed between the captured image and the registered image selected from the database (column 5 lines 17-21, lines 27-42 and FIG. 10 steps 1002-1010).

In the same art of authentication between the card device and host reader, **Benhammou** discloses a security system wherein the security memory device for smart cards and the host device perform the mutual authentication before allowing the host reader to read/write information to the cards (abstract, [0008] lines 5-16, [0033] lines 13-20, and FIG. 6 steps 50-57).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the information processing apparatus further comprising: network communication means which communicates with a management server managing the communication target, via a predetermined network; and relay means which relays mutual authentication between the communication target and the management server via the network communication means and the near-distance communication means, wherein in accordance with a result of the mutual authentication, comparison is performed by the biological authentication means, or in accordance with a comparison result by the biological authentication means, the mutual authentication is relayed by the relay means*, as taught by **Kono** and **Benhammou**, in the personal identification system of **Yap** and **Bridgelall**, for the purpose of developing a personal identification system including the database to mange all the registered users.

4. **Claim 7 is rejected under 35 USC 103(a) as being unpatentable over Yap in view of Kono, Bridgelall and further in view of Endoh et al. (Endoh - US 2004/0022421) and Nick Bromer (Bromer – US 6,476,715 B1).**

As to **claim 7**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 2** except for the claimed limitations of *the information processing apparatus wherein the communication target is provided with a light source, the information processing apparatus further comprising: generation means which generates a flicker pattern to control a flickering state of the light*

source, and encryption means which encrypts the flicker pattern generated by the generation means, and the biological authentication means compares the flicker pattern with a luminance pattern of the biological data, which is detected by the biological sensor through the living body brought close to the predetermined position and emitted with light flickered in accordance with the flicker pattern from the light source in the communication target brought close to the predetermined position.

In the same art of performing the biological authentication, **Endoh** discloses a device with built-in LEDs used as the light source to capture the user blood vessel image in the authentication process ([0202] - [0213], [0215]-[0218] and FIG. 1).

In the same art of performing encrypted authentication, **Bromer** discloses land vehicle having its vehicle identification number encoded into the binary format and the flickering encoded identifier is displayed using the brake light of the vehicle (abstract, column 1 line 61 – column 2 line 4, and FIG. 2 the brake lamp 100). In addition, the detector is coupled to a database to record the vehicle identification number and detect the flickering pattern from the vehicle to perform the authentication to determine whether the vehicle is stolen or wanted (abstract, column 2 lines 5-13, lines 20-26, lines 33-44, and FIG. 2 the detector 200).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the information processing apparatus wherein the communication target is provided with a light source, the information processing apparatus further comprising: generation means which generates a flicker pattern to control a flickering state of the light source, and encryption means which encrypts the flicker pattern generated by the generation means, and the biological authentication means compares the flicker pattern with*

a luminance pattern of the biological data, which is detected by the biological sensor through the living body brought close to the predetermined position and emitted with light flickered in accordance with the flicker pattern from the light source in the communication target brought close to the predetermined position, as taught by **Endoh** and **Bromer**, in the personal identification of **Yap**, **Kono,** and **Bridgelall**, for the purpose of generating the biological data as the flickering patter using the light source and performing the biological authentication between the communication target and the authentication device.

5. **Claim 11 is rejected under 35 USC 103(a) as being unpatentable over Yap in view of Kono, Bridgelall and further in view of Endoh and Jerome H. Lemelson (Lemelson - US 4,189,712).**

As to **claim 11**, **Yap**, **Kono,** and **Bridgelall** disclose the limitations of **claim 9** except for the claimed limitations of *the information processing apparatus wherein the equipment means is constituted by a circular ring portion, and a light source which is provided on the ring portion and emits imaging light on the identification target at the predetermined portion, and the imaging light is guided to an imaging element provided on the communication target, through the living body brought close to the communication target.*

In the same art of performing personal identification, **Endoh** discloses a cell phone having the light source for emitting light and photographing the user blood vessel by the reflected light of the user palm of the hand ([0202]-[0204] and FIG. 12).

In the same art of performing authentication, **Lemelson** discloses a switch and lock activating system and method. Further, **Lemelson** discloses the finger ring that contains the

security code to operate the activating system (column 3 lines 23-40, column 4 lines 33-68, and column 5 lines 29-68).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to modify the personal identification system of **Yap**, **Kono,** and **Bridgelall** to include *the information processing apparatus wherein the equipment means is constituted by a circular ring portion, and a light source which is provided on the ring portion and emits imaging light on the identification target at the predetermined portion, and the imaging light is guided to an imaging element provided on the communication target, through the living body brought close to the communication target,* as taught by **Endoh** and **Lemelson**, for the purpose of providing variations of the personal identification system.

6. **Claim 12 is rejected under 35 USC 103(a) as being unpatentable over Yap in view of Kono, Bridgelall and further in view of Bromer.**

As to **claim 12**, **Yap, Kono,** and **Bridgelall** disclose the limitations of **claim 9** except for the claimed limitations of *the information processing apparatus wherein the imaging light is emitted, flickered in accordance with a flicker pattern supplied from the communication target, the flicker pattern is compared with a luminance pattern of images sequentially generated on the basis of the imaging light.*

In the same art of performing encrypted authentication, **Bromer** discloses land vehicle having its vehicle identification number encoded into the binary format and the flickering encoded identifier is displayed using the brake light of the vehicle (abstract, column 1 line 61 – column 2 line 4, and FIG. 2 the brake lamp 100). In addition, the detector is coupled to a database to record the vehicle identification number and detect the flickering pattern from the

vehicle to perform the authentication to determine whether the vehicle is stolen or wanted (abstract, column 2 lines 5-13, lines 20-26, lines 33-44, and FIG. 2 the detector 200).

Therefore, it would have been obvious to one of the ordinary skill in the art at the time of the claimed invention to include *the information processing apparatus wherein the imaging light is emitted, flickered in accordance with a flicker pattern supplied from the communication target, the flicker pattern is compared with a luminance pattern of images sequentially generated on the basis of the imaging light,* as taught by **Bromer**, in the personal identification system of **Yap**, **Kono**, and **Bridgelall**, for the purpose of performing the biological authentication using the blood vessel pattern generated by the light source and the luminance pattern detected by the sensor to determine whether the user is authenticated to use the service.

Citation of Pertinent Art

7. The prior are made of record and not relied upon is considered pertinent to applicant's disclosure:

a. Haper, US 2004/0162988 A1, discloses optical card based system for individualized tracking and record keeping.

b. Rietveld, US 2004/0108377 A1, discloses identification system.

c. Cudlitz, US H2120 H, discloses biometric personal identification credential system (PICS).

d. Gennaro et al., US 6,317,834 B1, discloses biometric authentication system with encrypted models.

e. Dietz et al., US 2004/0208632 A1, discloses the communication using bi-directional LEDs.

f. Endol et al., US 2005/0148876 A1, the system and method to identify and authenticate personnel using biometric data.

g. Kono et al., US 2004/0120556 A1, which discloses the method and system to obtain the personal identification and perform the authentication based on the registered identification and the personal identification.

h. Kuffner et al., US 2004/0179588 A1, which discloses the method and apparatus for processing device identification to improve security in communication system.

i. Piosenka et al., US 4,993,068, which discloses the method and system to obtain the personal identification and perform the authentication based on the registered identification and the personal identification.

j. Benhammou et al., US 2004/0059925, which discloses the bi-directional communication and authentication between the device and host.

k. Kinsella, US 2002/0150282, which discloses the method and system to obtain the fingerprint identification and perform the authentication based on the registered fingerprint identification and the fingerprint identification.

l. Nagasaka et al., US 2002/0184641 A1, which discloses the method and system to obtain the blood vessel identification and perform the authentication based on the registered blood vessel identification and the blood vessel identification.

m. Nagasaka et al., US 2003/0037264 A1, which discloses the method and system to obtain the blood vessel identification and perform the authentication based on the registered blood vessel identification and the blood vessel identification.

n. Norris, Jr, US 6,695,207 B1, which discloses the apparatus and methods for identifying and authenticating personnel using the biometric identification.

o. Hattori et al., US 2008/0258864 A1, which discloses the bi-directional communication and authentication between the RFID tag and the interrogator.

Response to Arguments

8. Applicant's arguments with respect to claims 1-7 and 9-12 as amended have been considered but are moot in view of the new ground(s) of rejection. See above rejection using additional prior art to address the amendment corresponding to applicant's arguments.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to QUANG PHAM whose telephone number is (571)-270-3668. The examiner can normally be reached on Monday - Thursday 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BENJAMIN LEE can be reached on (571)-272-2963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/QUANG PHAM/
Examiner, Art Unit 2612

/BENJAMIN C. LEE/

Supervisory Patent Examiner, Art Unit 2612